Identifying Passive UHF RFID Tags Using Signal Features at Different Tari Durations

Baha' A. Alsaify
Computer Science and Computer Engineering Department
University of Arkansas
Fayetteville, Arkansas 72701
Email: b19842003@yahoo.co.uk

Dale R. Thompson
Computer Science and Computer Engineering Department
University of Arkansas
Fayetteville, Arkansas 72701
Email: drt@uark.edu

Jia Di
Computer Science and Computer Engineering Department
University of Arkansas
Fayetteville, Arkansas 72701
Email: jdi@uark.edu

***Abstract*—In this work, we identify RFID tags based on their inherent signal features, which can be another level of security on top of the traditional way of demonstrating knowledge of a secret key. Identification is the process of discovering the true identity of an entity from the entire collection of similar entities and requires one-to-many matching. Passive UHF RFID tags are identified by their signal features. The backscattered signal is recorded and a set of features based on timing and/or power are extracted to create a fingerprint. A fingerprint consisting of timing and power features was less accurate than either a timing-only or power-only fingerprint. The fingerprint consisting of timing-only features was more accurate than the fingerprint consisting of power-only features. We propose to use a fingerprint consisting of timing-only features as another layer of security because the accuracy is better and the features are easier to measure.**

I. Introduction

Radio frequency identification (RFID) is currently used in applications such as inventory control, permitting entry into buildings and rooms, tracking assets, and contactless payment systems. There are several reasons for the increase in usage of RFID technology. First, passive RFID tags have low cost [1], [2]. Second, reading and communicating with an RFID tag does not require line-of-sight. In addition, RFID tags can be reprogrammed, which means that they can be reused once their original purpose is no longer valid. The fact that RFID tags can be reprogrammed means that all the data on the tag can be manipulated.

An RFID system has two major components: one or more readers (or interrogators) and tags. The purpose of the reader is to send commands to the tag over a wireless channel. Upon receiving the reader's commands, the tag decodes the transmission and responds with the appropriate data. RFID tags can be classified as passive, semi-passive, and active. RFID tags operate in different frequency bands such as low-frequency (LF), high-frequency (HF), and ultra-high frequency (UHF), depending upon the application. In this work, we focus on passive UHF RFID tags since they are the ones that are widely used by the industry. The protocol that is used to control the communication between the tags and the readers is known as EPC Class-1 Generation-2 (C1G2) or ISO/IEC 18000-6C [3].

Identification is the process of discovering the true identity of an item from the entire collection of similar items and requires one-to-many matching. In other words, the features of a tag are compared with previously enrolled tag features to determine the closest match. We refer to the vector of features as a fingerprint. In order to identify a tag, it must be enrolled in the system before using it in the real world. Authentication is the process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of the user/object with those previously proven, stored, and associated with the identity being claimed. Today, tags are authenticated by their Electronic Product Code (EPC), serialized transponder ID (TID) numbers [4], adding physical unclonable functions [5], [6], or by verifying stored secrets on the tag [7]. To provide a more secure way to authenticate and identify RFID tags, researchers propose to identify tags based on what they "are", not based on what they "have" [8], [9], [10]. In this work, we focus on identification based on the features of an RFID tag's signal. A sample of the tag's signal is shown in Fig. 1.

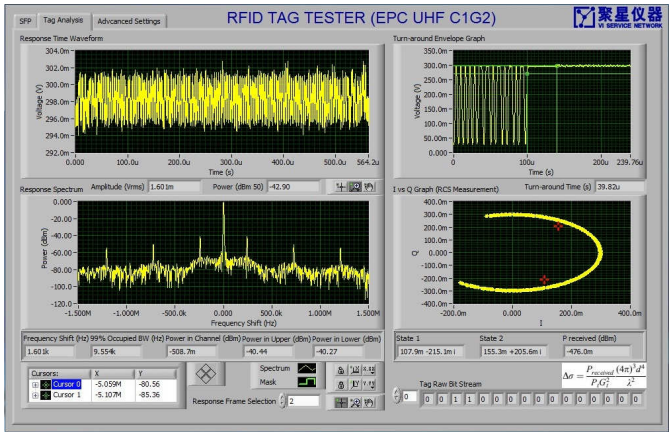

Fig. 1: RFID tag sample transmission.

In order to identify tags based on what they "are" rather than on what they "have", a set of features needs to be extracted from the tag. This set is stored in a vector that we call a fingerprint. In this paper, we compare power-and-

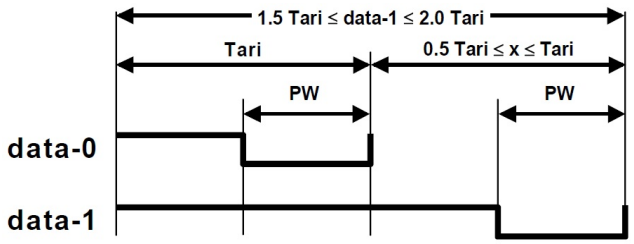

Fig. 2: Data encoded as Tari's.

timing, power-only, and timing-only fingerprints of UHF RFID tag signals. The contributions of this paper are to provide a study of the effectiveness of power and timing signal features on identification. Mainly, we are manipulating the type-A reference interval (Tari), which is a timing feature, that defines the duration of the zero symbol [11] and study its effect on the signal features.

The Tari is used as the reference time interval for the commands sent from the reader to the tag [3]. Fig. 2 shows how data-0 and data-1 will be encoded using a Tari. It shows that data-0 duration is equivalent to one Tari while data-1 duration can range between 1.5 and 2.0 Taris.

This paper is organized as follows. The next section provides an overview of the current related work in the area of identification. Section III provides the details of the experiments that are performed. The results of the experiments are provided in Section IV and finally the conclusions are discussed in Section V.

II. Related Work

The idea of identifying an object based on their physical features is not a new idea. Automatic human identification systems identify by features. First, humans were identified based on a numeric combination (key) they memorized. In order to have a more secure way to identify people, many systems that use human physical characteristics have been introduced [12], [13], [14], [15].

In this section, we discuss previous work on identifying RFID tags based on their signal features. Extracting timing and power features from the tag's transmitted signals and using them to identify the tag itself or the tag's manufacturer is proposed in [8], [9], and [10]. In [8], the authors fingerprint UHF RFID tags based on their minimum power response of the tags measured at multiple frequencies. To measure the minimum power response they use a bottom-up algorithm that sends signals to the tag. The power is slowly increased from a low value until the tag responds. When the tag response is detected, the power of the signal at that instant is recorded and is considered as the minimum power response. Frequencies that range from 860 MHz to 960 MHz are tested on 100 passive RFID tags. They show that both the frequency and the particular tag significantly affect the minimum power response. The authors use the k-Nearest Neighbor (k-NN) classifier based on the minimum power response. They are able to classify the tags with an average true positive rate (TPR) of 90.5% for two manufacturers.

Additional work on fingerprinting HF RFID tags is presented in [9]. The authors extract the modulation shape and spectral features of the signals emitted by RFID smart cards and RFID enabled passports subjected to well-formed reader commands and out-of-specification commands. The techniques are tested on a set of 50 RFID smart cards of the same manufacturer and model, and an undisclosed number of passports. All the experiments are performed in a controlled environment in which the reader and the tag are physically close. The classification experiments conducted on the passports show that modulation shaped features, burst features, and sweep spectral features have 0% error rate. On the other hand, using burst spectral features result in a 5.37% error rate which can be reduced to 4.69% using sweep spectral features. The features in [9] are measured in the HF frequency band and in the near field unlike our measurements that are from the UHF frequency band and in the far field. These techniques will not perform well over larger distances because HF tags use near-field communication. In addition, the measurements in [9] appear to be computationally intensive.

In [10], UHF RFID tag identification is discussed. A population of 70 passive UHF RFID tags from three different manufacturers are tested. The tag's location, orientation, and transmitted power are varied to build 10 experimental configurations. The extracted features are built by collecting the tag's RN16 preamble and each tag is queried 100 times in a noisy environment. Time-domain features that include time interval error (TIE) and average baseband power are collected. The results of the classification experiments show that TIE has an accuracy of 71.4% while the average baseband power has an accuracy of 43.2%. The experiments also show that combining them results in a 98.7% accuracy. In addition, it shows that the timing results are stable but the power results are not stable across different configurations. Finally, the spectral feature method from [9] is applied to UHF tags in [10] resulting in an accuracy of 99.6% but the results are not stable at varying distances.

Fingerprinting RFID tags by adding a random scattering structure to the tag is proposed in [6]. The additional structure renders a signal response that is unique and hard to replicate. The authors measure the near-field response of the added structure when creating the fingerprint. The reader and tag have to be very close, between 1mm and 8mm. A misalignment noise in the readings exists because of mounting issues. In order to verify that the fingerprint acquired works, a binary classification problem is assumed. Kernel Density Estimation is used to determine the underlying distribution of the fingerprints. The results of the classification show that the probability to confuse a fake tag with a real one is less than 10^{-200} if the same copper-based structure is used and that probability will be reduced to 10^{-300} considering all fingerprints. The disadvantage of this work is that the distance between the reader antenna and tag have to be very close when measuring the signal unlike in our work.

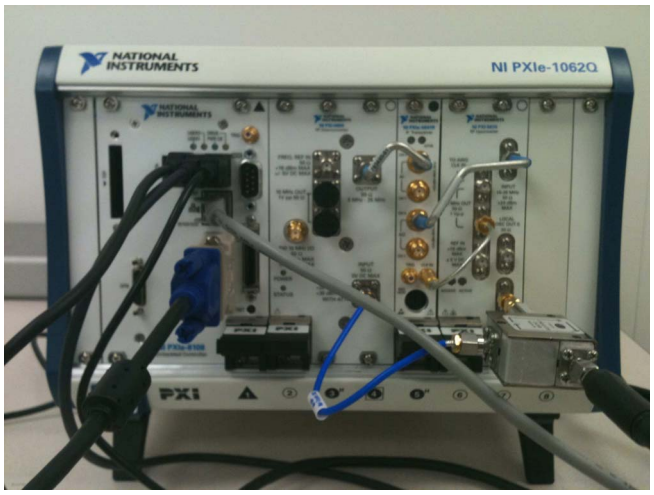

Fig. 3: Conformance test system.

Modifying the hardware of a tag in order to create a unique signal is suggested in [16]. The authors propose adding an analog circuit that performs some predefined mathematical operation on an analog signal. Their proposed system has the reader sending an analog signal simultaneously with the sent command but on a different carrier frequency. The tag accepts the signal and passes it to the special purpose analog circuit to perform the mathematical operation and returns the result to the reader. The reader then communicates with an authentication server to verify the results sent back by the tag. The ideas presented in the paper are interesting but no prototypes, simulations, or accuracy predictions are shown.

In order to put the work that we did in perspective, a comparison with the related work is provided in Table I.

III. Experiment Setup

We use a programmable reader that was built by [17] to measure RFID tag signal features. All the experiments are conducted in a noisy environment, where thermal noise, cell-phone noise, WiFi, and RF noise are present. During all the experiments, the distance between the tag and the reader's antenna is fixed for at 20 cm. For privacy purposes, the identity of the tag's manufacturer will not be presented. Instead we will refer to tag's manufacturer as A, B, or C. After each experiment run, the tag is assumed to have lost all of its stored energy, so that the next run will start with the tags having zero stored energy. The test system is shown in Fig. 3. This programmable test system can send valid or invalid commands, capture the tag responses, and provide signal features such as timing and power as shown in Fig. 1.

The tags are read in the far field range. We test 12 different tags from three manufacturers (4 tags per manufacturer). Each of the tested tags is queried using 3 different Tari values, 6.25μs, 12.5μs, and 25μs. For a fixed Tari duration, each tag is measured 5 times. In other words, each tag is measured 15 times, which makes the total number of measurements equal to 180.

Each of the tags is represented by a vector of features. These features can be categorized into three different groups:

- **Timing features** - These features correspond to the time it takes the tag to perform a certain task. There are two features in this group. First, the time it takes the tag to transmit its PC+EPC+CRC. Second, the time the tag needs to recharge after sending its PC+EPC+CRC data, which is known as T1. These features are measured in microseconds (μs);
- **Power features** - These features correspond to the different power readings that are associated with the PC+EPC+CRC transmission. There are three features that belong to this group. First, the received power of PC+EPC+CRC that is transmitted by the tag (PC+EPC+CRC Power). Second, the power received by the reader from the tag in an RF channel while the tag is transmitting the PC+EPC+CRC (power in channel). Finally, the power received by the reader from the tag in the channel below the measured RF channel while the tag is transmitting the PC+EPC+CRC (power in lower). All of the previous features are measured in dBm; and
- **Voltage features** - These features are extracted from the PC+EPC+CRC voltage-time waveform, which is shown in Fig. 1. There are two features in this group. The minimum voltage received by the reader from the tag and the variance of the voltage received by the reader from the tag. Both of the previous two features are measured in volts.

By looking at the previous list we can say that there is a total of seven features. Namely, these features are:

1) PC+EPC+CRC transmission time;
2) PC+EPC+CRC power;
3) Turn-around time (T1);
4) Power in channel;
5) Power in lower;
6) Voltage minimum in the transmitted PC+EPC+CRC; and
7) Voltage variance in the transmitted PC+EPC+CRC.

Two main experiments are conducted on the tag's captured signal features.

1) The variance in the collected data for each of the features is calculated. The variance is a measure of how far a group population is spread out. The variance is defined using Eqn. 1.

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2 \tag{1}$$

where μ is the group mean, N is the number of samples in the group, and x_i is the i^{th} sample. The purpose behind calculating the variance among tags that belong to the same manufacturer is to select features that have low variance. Out of each of the feature groups that are mentioned before, the feature with the least variance will be selected. The resultant feature vector will be used for classification purposes; and

TABLE I: Comparison with Related Work

	Freq.	Environment	# Tags	Performance
Proposed	UHF	uncontrolled	12	Tag Identification using timing features: Accuracy=97.22%, TPR=83.33% Tag Identification using power features: Accuracy=94.44%, TPR=67.67% Tag Identification using timing and power features: Accuracy=86.11%, TPR=16.67%
Periaswamy et al. 2010 [8]	UHF	controlled	100	Tag Identification Manufacturer 1 using power features: TPR=94.40% Tag Identification Manufacturer 2 using power features: TPR=90.70% Both Manufacturers: TPR=90.50%
Zanetti et al. 2010 [10]	UHF	uncontrolled controlled	70	Tag Identification using timing features: Accuracy=71.40% Tag Identification using power features: Accuracy=43.20% Tag Identification using power and timing features: Accuracy=98.70% Tag Identification using spectral features: Accuracy=99.60%
Lakafosis et al. 2011 [6]	UHF (8mm)	controlled	1 (multiple CoA)	Same CoA Error Probability: 10^{-200} All CoA's Error Probability: 10^{-300}
Danev et al. 2009 [9]	HF	controlled	50	Tag Identification using burst spectral features: TPR=92.67% Tag Identification using sweep spectral features: TPR=94.25%

2) Manufacturer and individual tag identification using timing, power, and voltage features. To identify a tag we use the classification technique k Nearest Neighbors (k-NN). k-NN is a technique that compares the test sample with a collection of previously known samples. k-NN calculates the distance between the test sample and the previously collected samples (training samples). Euclidean distance, hamming distance, and grey distance are some of the techniques that can be used to calculate distances. k-NN usually produces good results because it uses the training samples for comparisons instead of building a model. However, k-NN will take a long time to perform identification if the number of training samples is large. In addition, the memory requirement grows large when a large number of training samples is present.
Two metrics are used to quantify the performance of the k-NN classifier algorithm. The first metric is the True-Positive-Rate (TPR). TPR is a measure of how many positive predictions we have out of all positive samples as shown in Eqn. 2. Another metric is the classifier accuracy. The accuracy is a measure of the percentage of correct predictions out of all test samples. To calculate the accuracy we use Eqn. 3. All of the classification experiments are conducted using PRTools MatLab toolbox [18]. For more information regarding classification and pattern recognition, please refer to [19].

$$TPR = \frac{TP}{TP + FN} \tag{2}$$

$$accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{3}$$

As Eqn. 2 and Eqn. 3 show, there are four main counts needed for the calculations:

- **True Positive TP**: A count that describes the number of positive test samples that were correctly classified as positive;
- **False Positive FP**: A count that describes the number of negative test samples that were wrongly classified as positive;
- **True Negative TN**: A count that describes the number of negative test samples that were correctly classified as negative; and
- **False Negative FN**: A count that describes the number of positive test samples that were wrongly classified as negative.

IV. Results

As stated in Section III, we perform two sets of experiments. First, we calculate the variance of signal features to determine good features. Then, we perform identification by applying the k-NN classification algorithm.

A. Variance

Since we are testing three manufacturers, we present the results of the variance in three different tables, Table II, Table III, and Table IV. Each of the tables presents the variance results of one manufacturer. The features in each of the tables are numbered based on the feature list in Section III. Before calculating the variance among the different tags, we normalized all the data we have so that it is easier to compare the variance. To normalize the data we use Eqn. 4

$$normalized = \frac{x_i - min}{max - min} \tag{4}$$

where x_i is the data sample, min and max are the minimum and maximum values among a data group, respectively.

By looking at the data in Table II, Table III, and Table IV we notice the following:

1) Within the timing features group, T1's duration has less variance across different Tari's than PC+EPC+CRC transmission time;
2) Within the power feature group, the "Power in Channel" feature is the one with the lowest variance;
3) Within the voltage features group, both features have almost the same variance. We will choose to use the "voltage standard deviation" feature; and
4) Features within the voltage group have the highest variance among all groups.

TABLE II: Normalized variance in the features of the tags from manufacturer A.

Tari's Duration	$f1$	$f2$	$f3$	$f4$	$f5$	$f6$	$f7$
6.25μ**s**	0.1790	0.1461	0.1703	0.1373	0.1543	0.1578	0.1757
12.5μ**s**	0.1684	0.1428	0.1396	0.1382	0.2211	0.1776	0.1892
25.0μ**s**	0.2390	0.1438	0.1493	0.1640	0.2632	0.1752	0.1773

TABLE III: Normalized variance in the features of the tags from manufacturer B.

Tari's Duration	$f1$	$f2$	$f3$	$f4$	$f5$	$f6$	$f7$
6.25μ**s**	0.1757	0.1389	0.1492	0.1432	0.1583	0.1561	0.1536
12.5μ**s**	0.2526	0.1681	0.1721	0.1585	0.1684	0.1354	0.1698
25.0μ**s**	0.1465	0.1588	0.1761	0.1593	0.2211	0.1765	0.1678

TABLE IV: Normalized variance in the features of the tags from manufacturer C.

Tari's Duration	$f1$	$f2$	$f3$	$f4$	$f5$	$f6$	$f7$
6.25μ**s**	0.1458	0.1837	0.1745	0.1444	0.1381	0.2118	0.1767
12.5μ**s**	0.2605	0.1613	0.1393	0.1397	0.0947	0.1844	0.2128
25.0μ**s**	0.1363	0.1396	0.1696	0.1567	0.1967	0.1887	0.1843

TABLE V: **Manufacturer identification** confusion matrix when all features are used.

	Predicted Manufacturer		
Actual Manufacturer	**A**	**B**	**C**
A	2	0	2
B	1	2	1
C	0	1	3

TABLE VI: **Tag identification** results using all features.

	TPR	**Accuracy**
Manufacturer A	75.00%	50.00%
Manufacturer B	87.50%	75.00%
Manufacturer C	75.00%	50.00%
All Manufacturers	16.67%	86.11%

TABLE VII: **Manufacturer identification** confusion matrix when only timing features are used.

	Predicted Manufacturer		
Actual Manufacturer	**A**	**B**	**C**
A	4	0	0
B	0	4	0
C	0	0	4

TABLE VIII: **Tag identification** results using timing features.

	TPR	**Accuracy**
Manufacturer A	75.00%	87.50%
Manufacturer B	100.00%	100.00%
Manufacturer C	100.00%	100.00%
All Manufacturers	83.33%	97.22%

B. Classification

We use 1-NN to identify the manufacturer of the tag (manufacturer identification) and the individual tag (tag identification). The experiments use 80% of the available data to train the classifier and the remaining 20% of the data for testing purposes. Accuracy, TPR, and the confusion matrix are used to measure the performance of the 1-NN classifier.

1) All features with multiple Tari durations: The purpose of this experiment is to determine the accuracy of both manufacturer and tag identification when using all seven features at three different Tari durations. In other words, the signal of every tag is represented by 21 features, seven features at three different Tari durations. The confusion matrix for manufacturer identification is shown in Table V. The accuracy is calculated to be 72.22% using Eqn. 3, while the TPR is calculated to be 58.33% using Eqn. 2. Table VI shows the results of the tag identification problem. The first three rows include the results when identifying tags from a population of tags that are the same model and manufacturer. The final row includes the identification results when the tags used for training and testing are from all three manufacturers. For tag identification from a population of all three manufacturers, we can identify tags with an accuracy of 86.11% and a TPR of 16.67%.

2) Timing with multiple Tari durations: In this experiment, only timing features are used. The timing features include the time it takes the tag to transmit its PC+EPC+CRC data and the turn-around time (T1) for three different Tari durations. In other words, the signal of every tag is represented by 6 features. The confusion matrix for manufacturer identification is shown in Table VII. The accuracy and TPR are both 100%. Table VIII shows the results of the tag identification problem. For tag identification from a population of all three manufacturers, we can identify tags with an accuracy of 97.22% and a TPR of 83.33%.

3) Power with multiple Tari duractions: Next, we classify the tags using only power features. In this experiment, the PC+EPC+CRC power, power in lower, and power received are used as features at three different Tari durations. In other words, the signal of every tag is represented by 9 features. The confusion matrix for manufacturer identification is shown in Table IX from which the accuracy is calculated to be 94.44% and the TPR is calculated to be 91.67%. Table X shows the results of the tag identification problem. For tag identification from a population of all three manufacturers, we can identify tags with an accuracy of 94.44% and TPR of 67.67%.

4) Voltage with multiple Tari durations: In this experiment, the voltage features that are extracted from the voltage-time

TABLE IX: **Manufacturer identification** confusion matrix when only power features are used.

	Predicted Manufacturer		
Actual Manufacturer	**A**	**B**	**C**
A	4	0	0
B	0	3	1
C	0	0	4

TABLE X: **Tag identification** results using power features.

	TPR	**Accuracy**
Manufacturer A	75.00%	87.50%
Manufacturer B	100.00%	100.00%
Manufacturer C	75.00%	87.50%
All Manufacturers	66.67%	94.44%

TABLE XI: **Manufacturer identification** confusion matrix when only voltage features are used.

	Predicted Manufacturer		
Actual Manufacturer	**A**	**B**	**C**
A	2	1	1
B	0	2	2
C	3	0	1

TABLE XII: **Tag identification** results using voltage features.

	TPR	**Accuracy**
Manufacturer A	50.00%	75.00%
Manufacturer B	25.00%	62.50%
Manufacturer C	50.00%	75.00%
All Manufacturers	08.33%	84.72%

waveform are used. The minimum voltage recorded for the PC+EPC+CRC is used along with the standard deviation of recorded voltage-time waveform at three different Tari durations. In other words, the signal of every tag is represented by 6 features. The confusion matrix for manufacturer identification is shown in Table XI. The accuracy is 61.11% and the TPR is 41.67%. Table XII shows the results of the tag identification problem. For tag identification from a population of all three manufacturers, we can identify tags with an accuracy of 84.72% and TPR of 8.33%, which is a significant decrease compared to using power and timing features.

5) Features with low variance: From the results that are obtained from the variance calculations in Section IV-A, three features are designated to have the lowest variance among their groups: Turn-around time (T1), power in channel, and voltage standard deviation. In this experiment, we use these features for manufacturer identification purposes. As before, we are using 80% of the data for training and the remaining 20% of the data for testing. The confusion matrix that resulted from using 1-NN is provided in Table XIII. The accuracy is calculated to be 72.22% while the TPR is equal to 58.33%. Table XIV shows the results of the tag identification problem. For tag identification from a population of all three manufacturers, we can identify tags with an accuracy of 87.50% and TPR of 25.00%.

6) Manufacturer Identification ROC Results: In order to further support the results that were obtained in the previous tests, receiver operating characteristics (ROC) curves are used

TABLE XIII: **Manufacturer identification** confusion matrix when only features with low variance are used.

	Predicted Manufacturer		
Actual Manufacturer	**A**	**B**	**C**
A	2	0	2
B	0	1	3
C	0	0	4

TABLE XIV: **Tag identification** results using features with low variance.

	TPR	**Accuracy**
Manufacturer A	50.00%	75.00%
Manufacturer B	75.00%	87.50%
Manufacturer C	50.00%	75.00%
All Manufacturers	25.00%	87.50%

TABLE XV: Area under ROC curves (AUC) for **manufacturer identification** problem.

Features Used	**AUC**
All Features	59.38%
Timing Features	100.00%
Power Features	100.00%
Voltage Features	53.13%
Features with low variance	84.38%

TABLE XVI: **Manufacturer identification** results summary.

Features Used	**AUC**	**TPR**	**Accuracy**
All Features	59.38%	58.22%	72.22%
Timing Features	100.00%	100.00%	100.00%
Power Features	100.00%	91.47%	94.44%
Voltage Features	53.13%	41.67%	61.11%
Features with low variance	84.38%	58.33%	72.22%

TABLE XVII: Individual **tag identification** results summary when all tags are combined.

Features Used	**TPR**	**Accuracy**
All Features	16.67%	86.11%
Timing Features	83.33%	97.22%
Power Features	66.67%	94.44%
Voltage Features	8.33%	84.72%
Features with low variance	25.00%	87.50%

for manufacturer identification. ROC curves give the observer the ability to determine how good a classifier is by calculating the area under the curve (AUC). Curves with large AUC reflect a good classifier performance. In other words, the larger the AUC the better the performance of the classifier. From ROC curves, we calculate the area under each of the curves and we present the data in Table XV. The timing and power features are best for manufacturer identification.

C. Results and Discussion

The experiments demonstrate that it is possible to identify a tag's manufacturer or an individual tag if the correct set of features are used. In all the experiments, we use features at different Tari durations. The results for manufacturer identification are summarized in Table XVI. The results for individual tag identification are summarized in Table XVII.

The results indicate that using either power or timing signal

features can achieve a relatively high accuracy, with slightly better results from using the timing features (higher accuracy). The results also show that using voltage signal features are not appropriate for identification. One might think that using all features (timing, power, and voltage) would improve the results because the set includes timing features, which has the best performance. However, including more features does not improve the performance but decreases it as seen in Table XVI and Table XVII. The reason behind the poor performance when using all features is contributed to a phenomenon called "curse of dimensionality" [20], which states that increasing the number of features does not necessarily result in better classifier performance. We think the higher variance from the power measurements decreases the accuracy. In addition, we anticipate that the power features will not be as stable as the timing features.

V. Conclusions And Future Work

In this paper, identifying RFID tag signals based on power-and-timing, power-only, and timing-only fingerprints are compared. Timing, power, and voltage features were extracted from the tags' transmitted signals and used to identify an individual tag and a tag's manufacturer. The results show that it is important to select the appropriate set of features for classification purposes. Using timing features at different Tari durations, yielded perfect manufacturer identification and the highest accuracy for this sample set. Power features will produce good results for both manufacturer and individual tag identification, but with lower accuracy than timing features. On the other hand, using voltage features extracted from the voltage-time waveform will have less accuracy. Increasing the number of features does not necessarily enhance the performance of the classifier.

We were able to obtain an accuracy of 97.22% by using timing features measured at different data rates, which is greater than the accuracy of 94.44% when using power-only features. Note, that this accuracy is greater than previous far-field measurements of timing and approaches previously published accuracies that use both timing and power features. See Table I for details. Therefore, we proposed to use timing features when fingerprinting RFID tags. Although the power-only fingerprint was comparable to the timing-only fingerprint, power-only features are more difficult to measure and we anticipate that power features are less stable than the timing features.

The experiments focus on identification, which is a one-to-many matching process. However, we propose that it could also augment or replace authentication systems in resource-constrained devices such as RFID tags. When presented with a tag, the EPC could be used to index the previously enrolled fingerprint and verify that the enrolled features match the measured features of the tag.

In the future, we intend to extend the work by increasing the number of tags used for training and testing the classifier. We do realize that the sample size is rather small. In addition, we will test which of the Tari durations will produce the best identification performance.

Acknowledgment

This material is based upon work supported by the National Science Foundation, CISE/CNS Trustworthy Computing program, under grant No. CNS-1053286.

References

[1] B. Kinsella, "What do RFID tags cost?" Sept. 2010.
[2] C. Swedberg, "High demand keeps tag prices steady," Sept. 2010.
[3] *EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communication at 860 MHz - 960 MHz Version 1.2.0*, http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf, EPCglobal Inc Std., Oct. 2008.
[4] M. Lehtonen, A. Ruhanen, F. Michahelles, and E. Fleisch, "Serialized TID numbers - a headache or a blessing for RFID crackers?" in *IEEE Intl Conf. RFID*, Apr. 2009, pp. 233–240.
[5] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications," in *IEEE Intl Conf. RFID*, Apr. 2008, pp. 58–64.
[6] V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. Tentzeris, G. DeJean, and D. Kirovski, "RFID-CoA: The RFID tags as certificates of authenticity," in *IEEE Intl Conf. RFID*, Apr. 2011, pp. 207–214.
[7] B. Yoon, M. Sung, S. Yeon, and H. Oh, "HB-MP++ protocol: an ultra light-weight authentication protocol for RFID system," in *IEEE Intl Conf. RFID*, Apr. 2009, pp. 186–191.
[8] S. Chinnappa Gounder Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Trans. Dependable and Secure Computing*, vol. 8, no. 6, pp. 938–943, Nov./Dec. 2011.
[9] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *Proceedings of the USENIX Security Symposium*, 2009.
[10] D. Zanetti, B. Danev, and S. Capkun, "Physical-layer identification of UHF RFID tags," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*, ser. MobiCom '10. New York, NY, USA: ACM, 2010, pp. 353–364. [Online]. Available: http://doi.acm.org/10.1145/1859995.1860035
[11] "Advanced RFID measurements: Basic theory to protocol conformance test," Sept. 2009.
[12] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 2, pp. 385–395, June 2011.
[13] F. Turroni, D. Maltoni, R. Cappelli, and D. Maio, "Improving fingerprint orientation extraction," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 1002–1013, Sept. 2011.
[14] H. Choi, K. Choi, and J. Kim, "Fingerprint matching incorporating ridge features with minutiae," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 2, pp. 338–345, June 2011.
[15] V. Kanhangad, A. Kumar, and D. Zhang, "A unified framework for contactless hand verification," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 1014–1027, Sept. 2011.
[16] G. S. Smith and M. Coetzee, "Analogue fingerprinting for passive RFID tags," in *Proceedings of the 2008 Third International Conference on Broadband Communications, Information Technology & Biomedical Applications*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 156–163. [Online]. Available: http://dl.acm.org/citation.cfm?id=1468167.1468472
[17] "NEXJEN systems," http://www.nexjen.com/, September 2011.
[18] R. P. W. Duin, *Patern Recognition Tools (PRTools)*, 4th ed., 2010.
[19] C. M. Bishop, *Pattern Recognition and Machine Learning*. Springer, 2006.
[20] A. Jain, R. Duin, and J. M., "Statistical pattern recognition: a review," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 4–37, Jan. 2000.